

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-033756

(43)Date of publication of application : 31.01.2002

(51)Int.Cl.

H04L 12/44

(21)Application number : 2000-218711

(71)Applicant : HITACHI LTD

(22)Date of filing : 14.07.2000

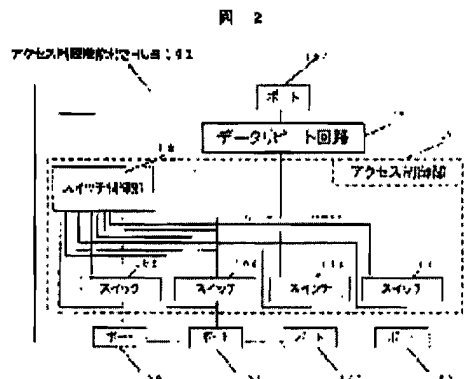
(72)Inventor : KODA SHUSAKU
TSURUTA HIROSHI

(54) HUB WITH ACCESS LIMIT FUNCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To solve the problems that conventionally a HUB, to which terminals are connected via routers, that the enhancement of the security of each terminal is indispensable to ensure the security of the terminals connected to the same HUB via the routers, that the security of all the terminals are endangered, once a manager right of the terminals is deprived, that the grouping of the terminals which are not communicating with each other into separate segments be required as the countermeasures and that expensive routers be required, when the number of the terminals increases resulting in complicated security rules described in the routers.

SOLUTION: The HUB itself is provided with a function, by which the direction and destination of data carried through each port can be discriminated to attain only communications between limited ports. Thus, by building up a scheme which will not to affect other terminals, even if the manager right of a terminal is deprived, the security for the terminals can be managed with few number of routers and without interactions occurring within the same segment.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-33756
(P2002-33756A)

(43)公開日 平成14年1月31日(2002.1.31)

(51)Int.Cl.⁷
H 0 4 L 12/44

識別記号

F I
H 0 4 L 11/00

テーマコード*(参考)
3 4 0 5 K 0 3 3

審査請求 未請求 請求項の数1 O L (全 5 頁)

(21)出願番号 特願2000-218711(P2000-218711)

(22)出願日 平成12年7月14日(2000.7.14)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 好田 秀作

神奈川県秦野市堀山下1番地 株式会社日立製作所エンタープライズサーバー事業部内

(72)発明者 ▲鶴▼田 啓

神奈川県秦野市堀山下1番地 株式会社日立製作所エンタープライズサーバー事業部内

(74)代理人 100075096

弁理士 作田 康夫

Fターム(参考) 5K033 CB08 DB03 DB18

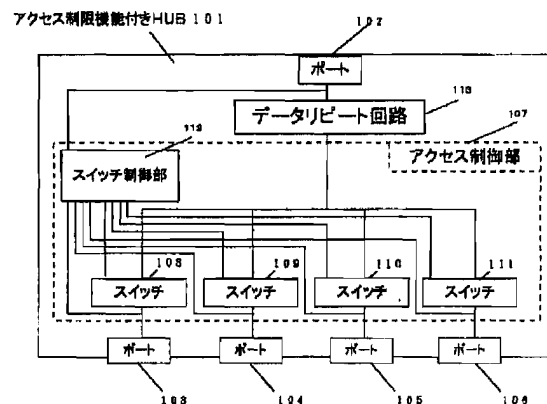
(54)【発明の名称】 アクセス制限機能付きHUB

(57)【要約】

【課題】ルータ経由で同一HUBに接続された端末のセキュリティ確保には、各端末のセキュリティの向上が不可欠であり、一旦端末の管理者権限が奪われるとその場の端末全てが危険にさらされる。この対策として相互に通信をしない端末同士は、ルータで個別のセグメントに分ける必要があった。また、端末の台数が増えてくると高価なルータが必要になりそこに記述するセキュリティルールも複雑なものになる。

【解決手段】HUB自体に各ポートを流れるデータの方角と行き先が判断できる機能を備え、限られたポート間の通信のみを可能にする。これにより、ある端末の管理者権限が奪われても、他の端末に影響を及ぼさない仕組みを構築することで、少ないルータで且つ、同一セグメントでの相互作用しない端末のセキュリティ管理が可能になる。

図 2



【特許請求の範囲】

【請求項1】 複数のポートと、各ポート間のデータを中継するためのデータリピータ回路とを備えるHUBにおいて、特定のポート間の通信のみ許可し、その他のポートとの通信を阻止する機能を有するアクセス制限機能付きHUB。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ローカルエリアネットワーク（LAN）において、複数の端末の間でデータを中継するために利用されるHUBに関するものであり、さらに詳しくは、特定のポート間の通信を制限することで、個々の端末のセキュリティを高めることができるHUBに関するものである。

【0002】

【従来の技術】従来、LANにおいてセキュリティ性を高める方法としては、ゲートウェイ（ファイアウォールを含む）、ルータやレイヤ3スイッチのアクセス制限機能により、特定のアドレスを持つ端末の通信を制御する方法が用いられている。図1はアクセス制限機能を有するゲートウェイ（ファイアウォールを含む）、ルータやレイヤ3スイッチの動作を示している。ゲートウェイ（ファイアウォールを含む）、ルータやレイヤ3スイッチに、端末の論理アドレス（例IPアドレス）と通信の許可・不許可を定義したアクセスリストを管理者が登録する。ゲートウェイ（ファイアウォールを含む）、ルータやレイヤ3スイッチはアクセスリスト中で、許可された通信のみを転送する。今、ポートPAに接続されたアドレスAを有する端末Taと、ポートPBに接続されたアドレスBを有する端末Tb間の通信は許可し、且つ、端末TbとポートPCアドレスCを有する端末Tcとの通信は不許可としたとする。管理者は通信を許可する端末のアドレスと通信の許可・不許可を定義したアクセスリストを、あらかじめルータやレイヤ3スイッチに登録しておく必要はない。さらにこのとき、各ポートに別々の論理ネットワークグループを設定する必要がある。

【0003】

【発明が解決しようとする課題】上述のように、ゲートウェイ（ファイアウォールを含む）、ルータやレイヤ3スイッチのアクセス制御機能を利用した方法は、設定の変更により柔軟にアクセス制限を定義できる利点がある。しかし、製品が高価であるという欠点を持っているうえに、ネットワークの構成が変わった場合などに、物理的な接続を変更する上にアクセス制限の設定を変更する作業が必要であるという煩わしさがともなう。

【0004】本発明は上述のような点に鑑みてなされたものであり、その目的とするところは、低コストでアクセスリスト作成の煩雑さが少なく、管理者権限を不正入手されることが無いアクセス制限機器を提供することにある。

【0005】

【課題を解決するための手段】本発明にあつては、上記の課題を解決するために、図2に示すように、複数のポート102、103、104、105、106と、各ポート間のデータを中継するためのデータリピータ回路113とを備えるHUB101において、各ポートのデータを中継するかしないかを制御するアクセス制御部107を有するものである。本発明の図2によれば、アクセス制御部107が、アクセス制限機能付きHUB101の各ポート103～106に接続される。アクセス制御部107は、ポート103～106と通信できるポート102と、ポート102とのみ通信できるポート103～106間の通信のみ転送する。また、その他のポート103～106間通信は転送しないよう動作することにより、特定のポート以外との通信ができないようにするものである。これにより、ユーザ（管理者）は端末のアドレスの登録や削除を一切行うことなく、アクセス制限を行うことができるものである。

【0006】

【発明の実施の形態】（実施形態1）図2は本発明の一実施例のブロック図である。それぞれのポート103～106毎にアクセス制御機構としてスイッチ108～111が接続されており、スイッチ108～111にはスイッチの動作を制御するスイッチ制御部112が接続されている。ポート103、104、105、又は106からポート102に向けてデータが流れる場合について動作を説明する。ポート103、104、105、又は106に受け取られたデータは、それぞれスイッチ108、109、110、または111で受取られると共にスイッチ制御部112に受け取られる。スイッチ制御部112はデータを受け取ったポートを識別し、データを受け取ったポートと接続されたスイッチを接続状態とし、それ以外のポートに接続されたスイッチを切断状態とする。これによりデータリピータ回路113のみにデータを送る。データリピータ回路はポート102にデータを送る。次にポート102からポート103、104、105、又は106に向けてデータが流れる場合について動作を説明する。ポート102が受け取ったデータは、データリピータ回路113を介して全てのスイッチ108～111に送られ、そのままポート103～106データが流れる。また、ポート102に流れたデータは、データリピータ回路113を介して全てのスイッチ108～111に送られ、ポート103、104、105、及び106に流れる。

【0007】図3は本実施例の動作説明図である。ポート102は他のすべてのポート103～106と通信可能であり、ポート103～106はポート102とのみ通信可能なポートである。例えば、ポート102からデータが送信されると図2のスイッチ108～111がすべてONになり、すべてのポートと通信可能となる。ポ

ート103にデータが送信されると、スイッチ108のみがONになり、ポート102とのみ通信可能となる。

【0008】(実施形態2)本発明のその他の一実施例について説明する。図2のブロック図において、それぞれのポート103～106毎にアクセス制御機構としてスイッチ108～111が接続されており、スイッチ108～111にはスイッチの動作を制御するスイッチ制御部112が接続されている。ポート103、104、105、又は106からポート102に向けてデータが流れる場合について動作を説明する。ポート103、104、105、又は106に受け取られたデータは、それぞれスイッチ108、109、110、または111で受取られると共にスイッチ制御部112に受け取られる。スイッチ制御部112はデータを受け取ったポートを識別し、データを受け取ったポートと接続されたスイッチを接続状態とし、それ以外のポートに接続されたスイッチを切断状態とする。これによりデータリピート回路113のみにデータを送る。データリピート回路はポート102にデータを送る。次にポート102からポート103、104、105、又は106に向けてデータが流れる場合について動作を説明する。ポート102が受け取ったデータは、スイッチ制御部112で宛先のポート103、104、105、又は106をチェックされ、該当するポートに接続されたスイッチのみを接続状態とし、それ以外のポートに接続されたスイッチを切断状態にすることにより、該当ポートのみに送られ、どのポート103～106にも該当しない場合そのデータは捨てられる。

【0009】(実施形態3)図4は、スイッチングHUBの応用によるアクセス制限機能付きHUB201である。各ポート202～206に対し各々を認識可能なアドレスを付加する、202～206に接続されていない外部からコントロールポート207に接続しアクセス制御部208にセキュリティポリシーを記述する。

【0010】アクセス制御部208は、アクセス制限機能付きHUB201の各ポート202～206を付加されたアドレスで認識しセキュリティポリシー設定された上で通信可能ポートだけのデータのやり取りを可能とする。コントロールポート207は、その他のいかなるポート202～206とも通信は出来ない。

【0011】本システムでは、CPU、メモリ等を設置し各ポート202～206に流れるデータを抽出し、TCP/IPのプロトコルを例に取れば発信元TCP、UDPポート番号と発信先TCP、UDPポート番号をチェックしパケットフィルタ型のファイアウォールの構築も可能になる。

【0012】

【発明の効果】本発明によれば、複数のポート間でデータを中継するためのHUBにおいて、特定のポート間の通信のみ許可し、その他のポートとの通信を阻止する機

能を有するアクセス制限機能を持たせることにより、ユーザによるアクセスリストの管理の必要を無くすることができ、また、特定のポートとの通信のみを許可することで、セキュリティ性を高めることができ、ルータやスイッチのアクセス制限機能を用いる方法より低コストで実現でき、ルータやスイッチの管理者権限を第三者に不正入手されることが無いという効果がある。インターネットに接続されたサーバでの設定例を元に効果の具体例を示す。

【0013】図5(a)では、端末がインターネットに提供しているサービスのアプリケーションにセキュリティ上の欠陥があり、端末の1つが管理者権限を奪われた場合、HUBの場合その他の端末も危険にさらされる。

【0014】この時ファイアウォールもしくはルータは何の役にも立たない。HUB接続されているイーサネット(登録商標)の速度で、攻撃が行われる。この対策としては個々に端末のセキュリティを向上させるしかない。技術的に高度であるし、台数分のセキュリティ対策が必要な為時間も掛かる。また、端末を直接操作できるサービスを提供しては、上記の環境では、他の端末に対し自由にアクセスできてしまう。図5(b)は図5(a)の対策型である。インターネットから端末に対してのアクセスを許可したい場合、セキュリティを考慮すると、各サービス毎にネットワークグループをファイアウォールもしくはルータで分割する必要がある。この場合、たとえ端末が乗っ取られた場合でも他の端末に影響を与えない。ネットワークグループ毎に、ネットワークインタフェースを設ける時ネットワークインタフェースの数は物理的に限界がある。

【0015】図5(c)は、アクセス制限機能付きHUBで構築した場合である。アクセス制限機能付きHUBは端末からファイアウォールもしくはルータに対してのアクセスを許可しても端末同士のアクセスを物理的に止めてしまう。インターネットから端末に対してのアクセスを許可したい場合、ルータやファイアウォールでアクセスコントロールを施せば、セキュリティHUBに接続されている端末が乗っ取られた場合でもセキュリティHUBを跨って、他の端末には攻撃が出来ない。また、ネットワークグループ毎に、ネットワークインタフェースを設ける必要が無い為コストが少なくて済む。

【図面の簡単な説明】

【図1】従来例の動作説明図である。

【図2】本発明の一実施例のブロック図である。

【図3】本発明の一実施例の動作説明図である。

【図4】スイッチングHUBを応用したアクセス制限機能付きHUBを示す図である。

【図5】アクセス制限機能付きHUBの使用例を示す図である。

【符号の説明】

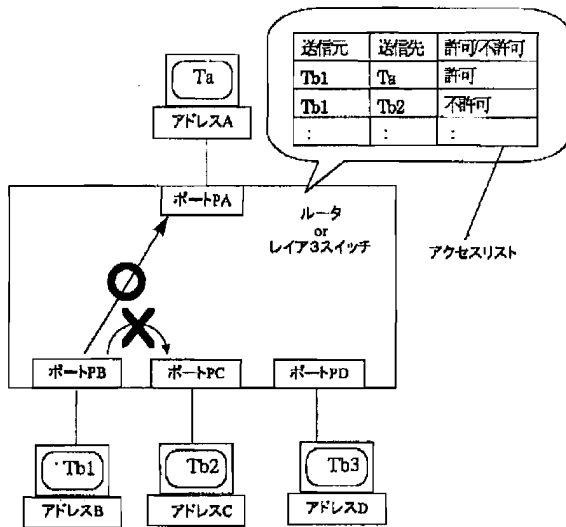
101…アクセス制限機能付きHUB、102～106

…HUBのポート、107…各ポートのデータの流を制御するアクセス制御部、108～111…HUBのポート103～106に流れるデータ処理するスイッチ、112…スイッチに流れたデータを制御するスイッチ制御部、113…データリピート回路、201…アクセス*

*制限機能付きHUB、202～206…HUBのポート、207…アクセス制御部を外部装置から制御するポート、208…HUBのポートに流れるデータを制御するアクセス制御部。

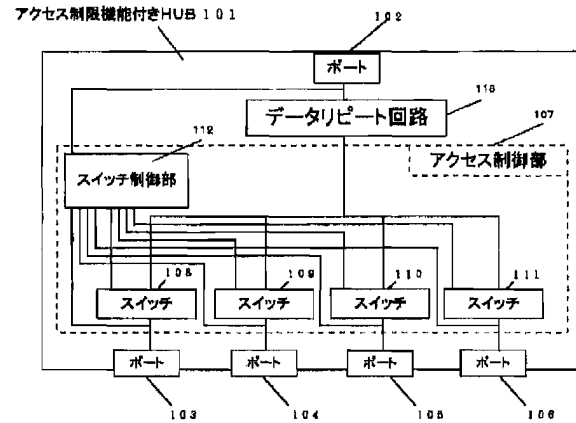
【図1】

図 1



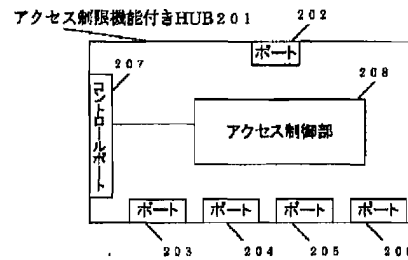
【図2】

図 2



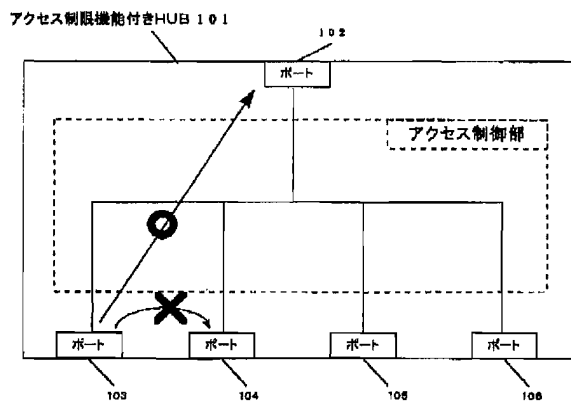
【図4】

図 4



【図3】

図 3



【図5】

図 5

